Chapter 2

Modular Forms of Level 1

In this chapter we study in detail the structure of level 1 modular forms, i.e., modular forms on $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(1) = \Gamma_1(1)$. We assume that you know some complex analysis (e.g., the residue theorem) and linear algebra, and have read Section 1.2.

2.1 Examples of Modular Forms of Level 1

In this section you will finally see some examples of modular forms of level 1! We will first introduce the Eisenstein series, one of each weight, then define Δ, which is a cusp form of weight 12. In Section 2.2 we will prove the structure theorem, which says that using addition and multiplication of these forms, we can generate all modular forms of level 1.

For an even integer $k \geq 4$, the *non-normalized weight k Eisenstein series* as a function on $\mathfrak{h}^*$ is

$$G_k(z) = \sum_{m,n\in\mathbb{Z}}^{*} \frac{1}{(mz+n)^k},$$

where for a given z, the sum is over all $m, n \in \mathbb{Z}$ such that $mz + n \neq 0$ (in particular, we omit nothing in the sum if $z \in \mathfrak{h}$).

Proposition 2.1.1. *The function $G_k(z)$ is a modular form of weight k, i.e., $G_k \in M_k(\mathrm{SL}_2(\mathbb{Z}))$.*

Proof. See [Ser73, § VII.2.3] for a proof that $G_k(z)$ defines a holomorphic function on $\mathfrak{h}^*$. To see that G_k is modular, observe that

$$G_k(z+1) = \sum^{*} \frac{1}{(m(z+1)+n)^k} = \sum^{*} \frac{1}{(mz+(n+m))^k} = \sum^{*} \frac{1}{(mz+n)^k},$$

where for the last equality we use that the map $(m, n+m) \mapsto (m, n)$ is invertible over $\mathbb{Z}$. Also,

$$\begin{aligned} G_k(-1/z) &= \sum^* \frac{1}{(-m/z+n)^k} \\ &= \sum^* \frac{z^k}{(-m+nz)^k} \\ &= z^k \sum^* \frac{1}{(mz+n)^k} = z^k G_k(z), \end{aligned}$$

where we use that $(n,-m) \mapsto (m,n)$ is invertible over $\mathbb{Z}$. □

Proposition 2.1.2. *$G_k(\infty) = 2\zeta(k)$, where ζ is the Riemann zeta function.*

Proof. In the limit as $z \to i\infty$ in the definition of $G_k(z)$, the terms involving z all go to 0 as $z \mapsto i\infty$. Thus

$$G_k(i\infty) = \sum_{n\in\mathbb{Z}}^* \frac{1}{n^k}.$$

This sum is twice $\zeta(k) = \sum_{n\geq 1} \frac{1}{n^k}$, as claimed. □

For example,

$$G_4(\infty) = 2\zeta(4) = \frac{1}{3^2 \cdot 5}\pi^4$$

and

$$G_6(\infty) = 2\zeta(6) = \frac{2}{3^3 \cdot 5 \cdot 7}\pi^6.$$

2.1.1 The Cusp Form Δ

Suppose $E = \mathbb{C}/\Lambda$ is an elliptic curve over $\mathbb{C}$, viewed as a quotient of $\mathbb{C}$ by a lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, with $\omega_1/\omega_2 \in \mathfrak{h}$. The *Weierstrass $\wp$-function* of the lattice Λ is

$$\wp = \wp_\Lambda(u) = \frac{1}{u^2} + \sum_{k=4,6,8,\ldots,\infty} (k-1)G_k(\omega_1/\omega_2)u^{k-2}.$$

It satisfies the differential equation

$$(\wp')^2 = 4\wp^3 - 60G_4(\omega_1/\omega_2)\wp - 140G_6(\omega_1/\omega_2).$$

If we set $x = \wp$ and $y = \wp'$ the above is an (affine) equation for an elliptic curve that is complex analytically isomorphic to $\mathbb{C}/\Lambda$. [[**Todo: See, e.g., Ahlfor's book.**]]

The discriminant of the cubic $4x^3 - 60G_4(\omega_1/\omega_2)x - 140G_6(\omega_1/\omega_2)$ is $16\Delta(\omega_1/\omega_2)$, where

$$\Delta = (60G_4)^3 - 27(140G_6)^2.$$

Since Δ is the difference of 2 modular forms of weight 12 it has weight 12. Morever,

$$\begin{aligned}\Delta(\infty) &= (60G_4(\infty))^3 - 27\,(140G_6(\infty))^2 \\ &= \left(\frac{60}{3^2\cdot 5}\pi^4\right)^3 - 27\left(\frac{140\cdot 2}{3^3\cdot 5\cdot 7}\pi^6\right)^2 \\ &= 0,\end{aligned}$$

so Δ is a cusp form of weight 12.

Lemma 2.1.3. *The only zero of the function Δ is at ∞.*

Proof. Let ω_1, ω_2 be as above. Since E is an elliptic curve, $\Delta(\omega_1/\omega_2) \neq 0$. □

2.1.2 Fourier Expansions of Eisenstein Series

Recall from (1.2.4) that elements f of $M_k(\mathrm{SL}_2(\mathbb{Z}))$ can be expressed as formal power series in terms of $q(z) = e^{2\pi i z}$, and that this expansion is called the Fourier expansion of f. The following proposition gives the Fourier expansion of the Eisenstein series $G_k(z)$.

Definition 2.1.4 (Sigma)**.** For any integer $t \geq 0$ and any positive integer n, let

$$\sigma_t(n) = \sum_{1\leq d|n} d^t$$

be the sum of the tth powers of the positive divisors of n. Also, let $\sigma(n) = \sigma_0(n)$, which is the number of divisors of n. For example, if p is prime then $\sigma_t(p) = 1 + p^t$.

Proposition 2.1.5. *For every even integer $k \geq 4$, we have*

$$G_k(z) = 2\zeta(k) + 2\cdot\frac{(2\pi i)^k}{(k-1)!}\cdot\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

Proof. See [Ser73, §VII.4], which uses a series of clever manipulations of series, starting with the identity

$$\pi\cot(\pi z) = \frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m} + \frac{1}{z-m}\right).$$

□

From a computational point of view, the q-expansion for G_k from Proposition 2.1.5 is unsatisfactory, because it involves transcendental numbers. For computational purposes, we introduce the *Bernoulli numbers* B_n for $n \geq 0$ *defined* by the following equality of formal power series:

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n\frac{x^n}{n!}. \tag{2.1.1}$$

Expanding the power series on the left we have

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \frac{x^2}{12} - \frac{x^4}{720} + \frac{x^6}{30240} - \frac{x^8}{1209600} + \cdots$$

As this expansion suggests, the Bernoulli numbers B_n with $n > 1$ odd are 0 (see Exercise 1.6). Expanding the series further, we obtain the following table:

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30},$$

$$B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2730}, \quad B_{14} = \frac{7}{6}, \quad B_{16} = -\frac{3617}{510}, \quad B_{18} = \frac{43867}{798},$$

$$B_{20} = -\frac{174611}{330}, \quad B_{22} = \frac{854513}{138}, \quad B_{24} = -\frac{236364091}{2730}, \quad B_{26} = \frac{8553103}{6}.$$

See Section 2.7 for a discussion of fast (analytic) methods for computing Bernoulli numbers. Use the `bernoulli` command to compute Bernoulli numbers in SAGE.

```
sage: bernoulli(12)
-691/2730
sage: bernoulli(50)
495057205241079648212477525/66
sage: len(str(bernoulli(10000)))
27706
```

For us, the significance of the Bernoulli numbers is that they are rational numbers and they are connected to values of ζ at positive even integers.

Proposition 2.1.6. *If $k \geq 2$ is an even integer, then*

$$\zeta(k) = -\frac{(2\pi i)^k}{2 \cdot k!} \cdot B_k.$$

Proof. The proof in [Ser73, §VII.4] involves manipulating a power series expansion for $z \cot(z)$. □

Definition 2.1.7 (Normalized Eisenstein Series)**.** The *normalized Eisenstein series* of even weight $k \geq 4$ is

$$E_k = \frac{(k-1)!}{2 \cdot (2\pi i)^k} \cdot G_k$$

Combining Propositions 2.1.5 and 2.1.6 we see that

$$E_k = -\frac{B_k}{2k} + q + \sum_{n=2}^{\infty} \sigma_{k-1}(n) q^n. \qquad (2.1.2)$$

It is thus now simple to explicitly write down Eisenstein series (see Exercise 2.1).

Warning 2.1.8. Our series E_k is normalized so that the coefficient of q is 1, but often in the literature E_k is normalized so that the constant coefficient is 1. We use the normalization with the coefficient of q equal to 1, because then the eigenvalue of the nth Hecke operator (see Section 2.4) is the coefficient of q^n. Our normalization is also convenient when considering congruences between cusp forms and Eisenstein series.

2.2 Structure Theorem For Level 1 Modular Forms

In this section we describe a structure theorem for modular forms of level 1. [[**Todo: Say something about general case at end of section. Eisenstein series still easier – see later in the book; modular symbols will be used to construct the cusp forms. Also point out somewhere what modular symbols useful for; e.g., a specific coefficient quickly (include my little paper about 144169!).**]] If f is a nonzero meromorphic function on $\mathfrak{h}$ and $w \in \mathfrak{h}$, let $\mathrm{ord}_w(f)$ be the largest integer n such that $f/(w-z)^n$ is holomorphic at w. If $f = \sum_{n=m}^{\infty} a_n q^n$ with $a_m \neq 0$, let $\mathrm{ord}_\infty(f) = m$. We will use the following theorem to give a presentation for the vector space of modular forms of weight k; this presentation will allow us to obtain an algorithm to compute a basis for this space.

Let $\mathcal{F}$ be the subset of $\mathfrak{h}$ of numbers z with $|z| \geq 1$ and $\mathrm{Re}(z) \leq 1/2$. This is the standard fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$. Let $\rho = e^{2\pi i/3}$.

Theorem 2.2.1 (Valence Formula)**.** *Suppose $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ is nonzero. Then*

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\,\mathrm{ord}_i(f) + \frac{1}{3}\,\mathrm{ord}_\rho(f) + \sum_{w\in\mathcal{F}}^{*} \mathrm{ord}_w(f) = \frac{k}{12},$$

where $\displaystyle\sum_{w\in\mathcal{F}}^{*}$ *is the sum over elements of $\mathcal{F}$ other than i or ρ.*

Proof. Serre proves this theorem in [Ser73, §VII.3] using the residue theorem from complex analysis. □

Let $M_k = M_k(\mathrm{SL}_2(\mathbb{Z}))$ denote the complex vector space of modular forms of weight k for $\mathrm{SL}_2(\mathbb{Z})$, and let $S_k = S_k(\mathrm{SL}_2(\mathbb{Z}))$ denote the subspace of weight k cusp forms for $\mathrm{SL}_2(\mathbb{Z})$. We have an exact sequence

$$0 \to S_k \to M_k \to \mathbb{C}$$

that sends $f \in M_k$ to $f(\infty)$. When $k \geq 4$ is even, the space M_k contains the Eisenstein series G_k and $G_k(\infty) = 2\zeta(k) \neq 0$, so the map $M_k \to \mathbb{C}$ is surjective. This proves the following lemma.

Lemma 2.2.2. *If $k \geq 4$ is even, then $M_k = S_k \oplus \mathbb{C}G_k$ and the following sequence is exact:*

$$0 \to S_k \to M_k \to \mathbb{C} \to 0.$$

Proposition 2.2.3. *For $k < 0$ and $k = 2$, we have $M_k = 0$.*

Proof. Suppose $f \in M_k$ is nonzero yet $k = 2$ or $k < 0$. By Theorem 2.2.1,

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum_{w\in D}^{*} \mathrm{ord}_w(f) = \frac{k}{12} \leq 1/6.$$

This is impossible because each quantity on the left-hand side is nonnegative so whatever the sum is, it is too big (or 0, in which case $k = 0$). □

Theorem 2.2.4. *Multiplication by Δ defines an isomorphism $M_{k-12} \to S_k$.*

Proof. (We follow [Ser73, §VII.3.2].) By Lemma 2.1.3 above Δ is not identically 0, so multiplication by Δ defines an injective map $M_{k-12} \hookrightarrow S_k$. To see that this map is surjective, we show that if $f \in S_k$ then $f/\Delta \in M_{k-12}$. Since Δ has weight 12 and $\mathrm{ord}_\infty(\Delta) \geq 1$, Theorem 2.2.1 implies that Δ has a simple zero at ∞ and does not vanish on $\mathfrak{h}$. Thus if $f \in S_k$ and we let $g = f/\Delta$, then g is holomorphic and satisfies the appropriate transformation formula, so $g \in M_{k-12}$. □

Corollary 2.2.5. *For $k = 0, 4, 6, 8, 10, 14$, the vector space M_k has dimension 1, with basis 1, G_4, G_6, E_8, E_{10}, and E_{14}, respectively, and $S_k = 0$.*

Proof. Combining Proposition 2.2.3 with Theorem 2.2.4 we see that the spaces M_k for $k \leq 10$ can not have dimension bigger than 1, since then $M_{k'} \neq 0$ for some $k' < 0$. Also M_{14} has dimension at most 1, since M_2 has dimension 0. Each of the indicated spaces of weight ≥ 4 contains the indicated Eisenstein series, so has dimension 1, as claimed. □

Corollary 2.2.6. $\dim M_k = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ \lfloor k/12 \rfloor & \text{if } k \equiv 2 \pmod{12}, \\ \lfloor k/12 \rfloor + 1 & \text{if } k \not\equiv 2 \pmod{12}, \end{cases}$ *where $\lfloor x \rfloor$ is the biggest integer $\leq x$.*

Proof. As we have seen above, the formula is true when $k \leq 12$. By Theorem 2.2.4, the dimension increases by 1 when k is replaced by $k + 12$. □

Theorem 2.2.7. *The space M_k has as basis the modular forms $G_4^a G_6^b$, where a, b are all pairs of nonnegative integers such that $4a + 6b = k$.*

Proof. Fix an even integer k. We first prove by induction that the modular forms $G_4^a G_6^b$ generate M_k, the cases $k \leq 12$ being clear (e.g., when $k = 0$ we have $a = b = 0$ and basis 1). Choose some pair of integers a, b such that $4a + 6b = k$ (these exist since k is even and $\gcd(4, 6) = 2$). The form $g = G_4^a G_6^b$ is not a cusp form, since it is nonzero at ∞. Now suppose $f \in M_k$ is arbitrary. Since $M_k = S_k \oplus \mathbb{C}G_k$, there is $\alpha \in \mathbb{C}$ such that $f - \alpha g \in S_k$. Then by Theorem 2.2.4, there is $h \in M_{k-12}$ such that $f - \alpha g = \Delta h$. By induction, h is a polynomial in G_4 and G_6 of the required type, and so is Δ, so f is as well.

Suppose there is a nontrivial linear relation between the $G_4^a G_6^b$ for a given k. By multiplying the linear relation by a suitable power of G_4 and G_6, we may assume that that we have such a nontrivial relation with $k \equiv 0 \pmod{12}$. Now divide the linear relation by $G_6^{k/12}$ to see that G_4^3/G_6^2 satisfies a polynomial with coefficients in $\mathbb{C}$. Hence G_4^3/G_6^2 is a root of a polynomial, hence a constant, which is a contradiction since the q-expansion of G_4^3/G_6^2 is not constant. □

Algorithm 2.2.8 (Basis for M_k)**.** *Given integers n and k, this algorithm computes a basis of q-expansions for the complex vector space M_k mod q^n. The q-expansions output by this algorithm have coefficients in $\mathbb{Q}$.*

1. [Simple Case] If $k = 0$ output the basis with just 1 in it, and terminate; otherwise if $k < 4$ or k is odd, output the empty basis and terminate.
2. [Power Series] Compute E_4 and E_6 mod q^n using the formula from (2.1.2) and the definition (2.1.1) of Bernoulli numbers.[[**Todo: Add reference to section on fast computation of Bernoulli numbers.**]]
3. [Initialize] Set $b = 0$.
4. [Enumerate Basis] For each integer b between 0 and $\lfloor k/6 \rfloor$, compute $a = (k-6b)/4$. If a is an integer, compute and output the basis element $E_4^a E_6^b$ mod q^n. When we compute, e.g., E_4^a, do the computation by finding $E_4^m \pmod{q^n}$ for each $m \le a$, and save these intermediate powers, so they can be reused later, and likewise for powers of E_6.

Proof. This is simply a translation of Theorem 2.2.7 into an algorithm, since E_k is a nonzero scalar multiple of G_k. That the q-expansions have coefficients in $\mathbb{Q}$ follows from (2.1.2). □

Example 2.2.9. We compute a basis for M_{24}, which is the space with smallest weight whose dimension is bigger than 1. It has as basis E_4^6, $E_4^3E_6^2$, and E_6^4, whose explicit expansions are

$$\begin{aligned} E_4^6 &= \frac{1}{191102976000000} + \frac{1}{132710400000}q + \frac{203}{44236800000}q^2 + \cdots \\ E_4^3E_6^2 &= \frac{1}{3511517184000} - \frac{1}{12192768000}q - \frac{377}{4064256000}q^2 + \cdots \\ E_6^4 &= \frac{1}{64524128256} - \frac{1}{32006016}q + \frac{241}{10668672}q^2 + \cdots \end{aligned}$$

In Section 2.3, we will discuss properties of the reduced row echelon form of any basis for M_k, which have better properties than the above basis.

2.3 The Victor Miller Basis

Lemma 2.3.1 (Victor Miller)**.** *The space S_k has a basis $f_1, \ldots, f_d$ such that if $a_i(f_j)$ is the ith coefficient of f_j, then $a_i(f_j) = \delta_{i,j}$ for $i = 1, \ldots, d$. Moreover the f_j all lie in $\mathbb{Z}[[q]]$.*